section 8

interfaces the intelligent interconnecting device 1 with the personal computers 2 as terminals.

The storage section 9 stores therein various programs to be executed by the central controlling section 6 and also stores data therein which is given thereto and is to be sent out therefrom via the LAN trunk line interfacing section 7 and the port interfacing section 8. The storage section 9 has a storage area whose storage content is not erased even when the power supply is cut off and a storage area whose storage content is erased when the power supply is cut off so that data is selectively stored in the respective areas according to its use and so on. The storage section 9, which is realizable by a generally known storage element and therefore, is not explained in detail, is appropriately structured, for example, by using a hard disk and the like as well as a semiconductor memory such as what is called an RAM and an ROM, and the like.

【0017】 Note that, according to the embodiment of the present invention, a TCP/IP protocol is stored in the area of the storage section 9 whose storage content is not erased even when the power supply

is cut off, and it is executed by the central controlling section 6 when necessary. Incidentally, among various TCP/IP protocols, any TCP/IP protocol may be used as long as it is appropriate for executing the unauthorized access avoiding processing, which is described later, and more specifically as long as it carries out what is known as authentication processing by using a user identifier and a password.

Moreover, in the storage section 9, an IP address given in advance to the intelligent interconnecting device 1, and a user identifier (ID) and a password necessary for authentication of an access from an external apparatus based on the TCP/IP protocol are stored in advance in the area whose content is not erased even when the power supply is cut off.

【0018】 A first example of the unauthorized access avoiding processing executed by the central controlling section 6 is explained next with reference to FIG. 3.

To explain first, it is premised that the unauthorized access avoiding processing is executed as one step of subroutine processing in main routine processing executed in the central

controlling section 6.

When the central controlling section 6 starts the processing, it is first judged whether or not an access from outside has occurred to the intelligent interconnecting device 1 (refer to a step S100 in FIG. 3). When it is judged that the access from outside has occurred (YES), the procedure proceeds to a next step S102. Meanwhile, when it is judged in the step S100 that no access from outside has occurred (NO), this subroutine processing is once finished, the procedure returns to the not shown main routine processing, and this subroutine processing is started again after predetermined processing of the main routine processing.

【0019】 Then, in the step S102, it is judged whether or not the access to the intelligent interconnecting device 1 from outside is a first access. When the access is judged to be the first access (YES), the procedure proceeds to a next step S110. Meanwhile, when the access is not judged to be the first access (NO), the procedure proceeds to a later described step S104.

In the step S110, a user identifier (ID) and a password are demanded from an external apparatus